

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-016255
 (43)Date of publication of application : 19.01.2001

(51)Int.CI.

H04L 12/56
 H04L 12/46
 H04L 12/28
 H04L 12/66

(21)Application number : 11-183067

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 29.06.1999

(72)Inventor : TERAO KAZUYUKI
 ONO SATOSHI

(54) INTER-NETWORK COMMUNICATION METHOD AND SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To operate physically one server as if each closed area network had a server in the communication between a plurality of the closed area networks and a server side network.

SOLUTION: In this communication method, when an access server AS has a point-to-point protocol PPP connection request from a terminal in a closed area network to a server, which PPP line in which closed area network is identified, a corresponding line is selected in an address space (Figure B) at a server side assigned in advance by PPP lines of closed area networks, an address of a terminal of the closed area network is made to correspond to the selected line (Figure A), address conversion is applied to a packet and the packet is sent to the server side network. The packet from the server side network is address converted by referring to the Figure A, which PPP line in which closed area network is recognized and the packet is sent to the line.

	FIGURE A	FIGURE B	SERVER SIDE NETWORK
CLIENT	アドレス1	---	アドレス1
CLIENT	アドレス2	---	アドレス2
CLIENT	アドレス3	---	アドレス3
CLIENT	---	アドレス4	アドレス4 (選択)
CLIENT	---	アドレス5	アドレス5
CLIENT	---	アドレス6	アドレス6
SERVER	アドレス10	アドレス10	アドレス10

	FIGURE A	FIGURE B
CLIENT 1	アドレス範囲: 01-300	アドレス範囲: 01-300
CLIENT 2	アドレス範囲: 301-600	アドレス範囲: 301-600
CLIENT 3	アドレス範囲: 601-900	アドレス範囲: 601-900
CLIENT 4	アドレス範囲: 901-1200	アドレス範囲: 901-1200

LEGAL STATUS

[Date of request for examination] 29.06.1999

[Date of sending the examiner's decision of rejection] 15.10.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3394727

[Date of registration] 31.01.2003

[Number of appeal against examiner's decision of rejection] 2002-21936

[Date of requesting appeal against examiner's decision of rejection] 13.11.2002

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-16255

(P2001-16255A)

(43)公開日 平成13年1月19日 (2001.1.19)

(51)Int.Cl.
H 04 L 12/56
12/46
12/28
12/66

識別記号

F I
H 04 L 11/20
11/00
11/20

テマコト[®](参考)
1 0 2 D 5 K 0 3 0
3 1 0 C 5 K 0 3 3
B

審査請求 有 請求項の数13 O.L (全20頁)

(21)出願番号 特願平11-183067
(22)出願日 平成11年6月29日(1999.6.29)

(71)出願人 000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(72)発明者 寺尾 和幸
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内
(72)発明者 小野 諭
東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内
(74)代理人 100066153
弁理士 草野 卓 (外1名)
Fターム(参考) 5K030 GA15 HD08 HD09 KA01 KA04
5K033 BA04 CB09 CC01 DA06 DB12

(54)【発明の名称】 ネットワーク間通信方法及びその装置

(57)【要約】

【課題】複数閉域網とサーバ側ネットワークとの間の通信で、物理的に1台のサーバを各閉域網にそれぞれサーバがあるかのように動作させる。

【解決手段】閉域網の端末からサーバへのPPP接続要求がアクセスサーバASにあると、どの閉域網のどのPPP回線であるかを識別し、閉域網のPPP回線ごとに予め割り当てたサーバ側のアドレス空間(図2B)の中から対応する1つを選択して、その閉域網の端末のアドレスを対応付け(図2A)、パケットをこのアドレス変換を行ってサーバ側ネットワークへ送る。サーバ側ネットワークからのパケットを、図2Aを参照してアドレス変換と共に、どの閉域網のどのPPP回線かを知り、その回線にパケットを送る。

	A		
	閉域網 A	閉域網 B	サーバ側ネットワーク
ホスト1	アドレス1	—	アドレス101
ホスト2	アドレス2	—	アドレス220
ホスト3	アドレス3	—	アドレス102
ホスト4	—	アドレス11	アドレス301(静的)
ホスト5	—	アドレス22	アドレス321
Server	アドレス100	アドレス150	アドレス1

	A	B
割り当て空間	アドレス空間101-300	アドレス空間301-350
PPP回線1	アドレス空間101-200	アドレス空間311-350
PPP回線2	アドレス空間201-250	アドレス301
動的割り当て	アドレス空間251-300	—

【特許請求の範囲】

【請求項1】 複数のユーザ側ネットワークのそれぞれとサーバ側ネットワークとをPPP (Point-to-Point Protocol)を利用して接続して通信を行う方法において、PPP接続確立時に、そのPPP回線が所属するユーザ側ネットワークを認証し、
 サーバ側ネットワークで、予め各ユーザ側ネットワークごとにそれぞれ割り当てた複数のアドレス空間における、上記認証したネットワーク及びPPP回線に対するアドレス空間から選んだアドレスに、そのユーザ側ネットワークのPPP回線からのパケットのアドレスを変換してそのパケットをサーバ側ネットワークへ送り、かつその変換アドレスと変換前のアドレスと、認証したユーザ側ネットワーク及びPPP回線との対応表を記憶しておき、
 サーバ側ネットワークからのパケットのアドレスを上記対応表を参照して上記アドレス変換の逆変換を行って対応するユーザ側ネットワークのPPP回線へ送ることを特徴とするネットワーク間通信方法。

【請求項2】 上記アドレス変換の際に、上記ユーザ側ネットワークからのパケットのデスティネーションアドレスをサーバ側ネットワークにおける該当するアドレスに変換することを特徴とする請求項1記載のネットワーク間通信方法。

【請求項3】 上記アドレス変換の際に、上記ユーザ側ネットワークからのパケットのサーバに対するポート番号を、そのユーザ側ネットワークに固有のポート番号に変換することを特徴とする請求項1又は2記載のネットワーク間通信方法。

【請求項4】 上記アドレスの選択はユーザ側ネットワークの利用方針に応じて動的又は静的に行うことを行なうことを特徴とする請求項1乃至3の何れかに記載のネットワーク間通信方法。

【請求項5】 上記PPP接続が確立した後にそのPPP回線からのパケットは、そのアドレスにて上記対応表を参照してアドレス変換して、サーバ側ネットワークへ送信することを特徴とする請求項1乃至4の何れかに記載のネットワーク間通信方法。

【請求項6】 複数のユーザ側ネットワークのそれぞれとサーバ側ネットワークとをPPP (Point-to-Point Protocol)を利用して接続して通信を行う方法において、PPP接続確立時に、そのPPP回線が所属するユーザ側ネットワークを認証し、
 予め各ユーザ側ネットワークのPPP回線毎に割り当てたVLAN (virtual LAN) を利用する時に利用するVLANを識別する情報を、上記認証されたユーザ側ネットワークのPPP回線よりのパケットに付加してサーバ側ネットワークへ送り、
 サーバ側ネットワークからのパケットのVLANを識別する情報から求めたユーザ側ネットワークのPPP回線 50

にそのパケットを送ることを特徴とするネットワーク間通信方法。

【請求項7】 複数ユーザ側ネットワークのそれぞれとサーバ側ネットワークとをPPP (Point-to-Point Protocol)を利用して接続して通信を行う方法において、PPP接続確立時に、そのPPP回線が所属するユーザ側ネットワークを認証し、
 予め各ユーザ側ネットワークごとに割り当てたVLAN (virtual LAN) を利用する時に利用するVLANを識別する情報を、上記認証されたユーザ側ネットワークのPPP回線よりのパケットに付加してサーバ側ネットワークへ送り、
 かつそのパケットのアドレスとVLANを識別する情報とPPP回線との対応表を記憶しておき、
 サーバ側ネットワークからのパケットのVLANを識別する情報及びアドレスから上記対応表を参照してPPP回線を求めて、そのパケットをユーザ側ネットワークのそのPPP回線に送ることを特徴とするネットワーク間通信方法。

【請求項8】 複数のユーザ側ネットワークとPPP (Point-to-Point Protocol)により接続されるサーバ側ネットワークとの間に設けられるアクセスサーバ装置であって、

各ユーザ側ネットワークのPPP回線ごとに割り当てられたアドレス空間を記憶するアドレス空間割り当てテーブルと、

接続してくる端末がどのユーザ側ネットワークのどのPPP回線に属するかの認証を行う手段と、

上記認証されたユーザ側ネットワークのPPP回線に対し、上記アドレス空間割り当てテーブルで割り当てられている1つのアドレスに、上記PPP回線よりのパケットのアドレスを変換してそのパケットをサーバ側ネットワークへ送るアドレス変換手段と、

上記アドレス変換されたアドレスと変換前のアドレスとの関係を記憶する変換アドレス記憶手段と、

サーバ側ネットワークからのパケットのアドレスを上記変換アドレス記憶手段を参照して変換し、かつ上記テーブルを参照して対応するユーザ側ネットワークのPPP回線へそのパケットを送るアドレス逆変換手段とを具備するアクセスサーバ装置。

【請求項9】 ユーザ側ネットワークのPPP回線からのパケットを、そのアドレスにより上記変換アドレス記憶手段を参照してアドレス変換してサーバ側ネットワークへ送る手段を備えることを特徴とする請求項8記載のアクセスサーバ装置。

【請求項10】 上記アドレス変換手段はパケットのデスティネーションアドレスをサーバ側ネットワークの該当するアドレスに変換する手段を備えることを特徴とする請求項8又は9記載のアクセスサーバ装置。~

【請求項11】 上記アドレス変換手段は、パケット中

3

のサーバに対するポート番号を、そのユーザ側ネットワークに固有のポート番号に変換する手段も備えることを特徴とする請求項8乃至10の何れかに記載のアクセスサーバ装置。

【請求項12】複数のユーザ側ネットワークとPPP (Point-to-Point Protocol)により接続されるサーバ側ネットワークとの間に設けられるアクセスサーバ装置であって、

ユーザ側ネットワークのPPP回線とVLAN (virtual LAN) を利用する時に利用するVLANを識別する情報との関係を記憶したVLAN識別情報テーブルと、

PPP接続確立時に、そのPPP回線がどのユーザ側ネットワークに属するかの認証を行う手段と、

上記認証されたユーザ側ネットワークのPPP回線と対応するVLANを識別する情報を、上記テーブルを参照して求め、上記PPP回線よりのパケットに付加してサーバ側ネットワークへ送る手段と、

サーバ側ネットワークよりのパケットを、そのVLANを識別する情報から上記テーブルを参照して対応するユーザ側ネットワークのPPP回線へ送る手段とを具備するアクセスサーバ装置。

【請求項13】複数のユーザ側ネットワークとPPP (Point-to-Point Protocol)により接続されるサーバ側ネットワークとの間に設けられるアクセスサーバ装置であって、

ユーザ側ネットワークとVLAN (virtual LAN) を利用する時に利用するVLANを識別する情報との関係を記憶したVLAN識別情報テーブルと、

PPP接続確立時に、そのPPP回線がどのユーザ側ネットワークに属するかを認証する手段と、

上記認証されたユーザ側ネットと対応するVLANを識別する情報を上記テーブルを参照して求め、上記PPP回線よりのパケットに付加してサーバ側ネットワークへ送る手段と、

上記パケットのアドレスと、上記VLANを識別する情報と上記PPP回線との対応表を記憶する手段と、

サーバ側ネットワークよりのパケットを、そのVLANを識別する情報とアドレスとから、上記テーブル及び上記対応表を参照して対応するユーザ側ネットワークのPPP回線へ送る手段とを具備するアクセスサーバ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は異なる複数のネットワーク、特に閉域網間の通信を行うエクストラネット向けの共有サーバのホスティングサービス（各ユーザ側ネットワークに貸出すサービス）の提供や、チケット予約サービスなどパブリックなサービスをこれらのユーザ側ネットワーク（閉域網）上のサーバの持つ情報を組み込むことによりユーザ側ネットワーク（閉域網）単位でカスタマイズした（各ユーザ側ネットワークのニーズに

4

応じた）サービスを安全に提供するなど電子商取り引きを含めた情報流通通信方法及びその装置に関する。

【0002】

【従来の技術】今日インターネットを始めネットワークの利用は広く普及し、多くの企業においては企業内の通信費用を安く抑えかつ、安全に行うために閉域網の構築を行っている。この構築においては、専用線だけでなくATM、FR（フレームリレー）を用いたり、IP（インターネットプロトコル）トンネリングを利用して行っている。また、営業マンなどが外出先からこれらの閉域網に接続する場合には、PPP (Point-to-Point Protocol)やその拡張であるL2TP (Layer2 tunneling Protocol)を用いている。閉域網間の通信が今後増加し、複数の閉域網で利用する共用サーバを自閉域網の閉域性を失うことなく提供したり、チケット予約サービスなどのパブリックなサービスを、各閉域網上のサーバの持つ情報を組み合わせてカスタマイズしての利用が増える。これの実現方法として、各閉域網上にサービスを提供するサーバを用意する方法があるがこれはコストがかかり、サーバを用意する側の負担が大きい。そこで、物理的には1台のサーバであるが、各閉域網からは各自別のサーバが存在するように見え、カスタマイズしたサービスをセキュア（安全）に提供できる仮想プライベートサーバの構築を考える。

【0003】現在、企業などの閉域網の構築においては、ネットワークの急激な普及によるIPアドレスの不足のために、ローカルアドレスを用いるか、インターネットなど外部に接続する時にのみ動的にグローバルアドレスを付与して外部と通信を行う方法が取られている。

しかし、動的にアドレスを付与する場合、次回の接続時には同一のアドレスを付与されると限らないので、特に移動端末など必要時にしか接続しない／その接続自体が不安定である場合、静的にアドレスを付与することがより必要となる。また、動的にアドレスを付与する状況ではサーバ側から特定の端末への接続確立は困難であるので、ネットワーク構築時にローカルアドレスを静的に付与する場合が多い。物理的に1台のサーバでこのように構築されている閉域網に対してのサービス提供を考えた場合、（1）サーバ側ネットワークを介した不正な接続など防止、（2）接続している閉域網間におけるアドレス空間の衝突、（3）サーバから移動端末を含めた特定の端末への接続確立、という3つの問題の解決が必要となる。

【0004】このサーバの構築には、既存技術のL2TP (Layer2 tunneling Protocol)に代表されるPPPトンネリング技術、NAT (Network Address Translation)に代表されるアドレス変換技術の2種類が有用な技術であるといえる。まず、PPPトンネリング技術により移動端末は時間と場所に制約されずに常に自分の閉域網への接続が可能になり、あたかもその閉域網に存在し

5

ているかのように閉域網の利用が可能になる。また、図22に示すように閉域網A、Bがインターネット／公衆網を介してサーバ側ネットワークと接続可とされ、各閉域網A、Bに属するホスト（端末とも云う）にはそれぞれのローカルアドレス空間A、Bでのアドレスが与えられており、各ホストはそれが属する閉域網の網間アクセスサーバ（AS）を通じ、PPPトンネリングを利用してサーバ側ネットワークの網間アクセスサーバと接続してサーバと接続可能とされている。この構成により、PPP接続をサーバ側までトンネリングすることで端末に、あたかも自分の閉域網に属するサーバと接続しているように見せることができる。これにより、閉域網の持つ閉域性を維持したり、閉域網で割り当てられているローカルアドレスをそのまま使用することが可能になる。しかし、

（1）閉域網では端末にローカルアドレスを自由に割り当てるので、複数の異なる閉域網に属する端末が同一のアドレスを持つ場合が生じ、この場合は衝突が避けられない。そのため、接続先のサーバ側ネットワークから見ると同一のアドレスを持つ端末が複数存在することが発生し、この時どの端末と通信しているかを正しく認識することが出来ない。

【0005】（2）サーバを示すアドレスを各閉域網で共通にする必要があり既存の設備への大幅な変更が必要になる場合がある。

（3）端末からの接続確立時にサーバ側からアドレスを動的に割り当てる場合、移動端末のように必要に応じてネットワークに接続してくる端末にはどのアドレスが割り当られているか不明であって、有用なサービスであるサーバ側からの情報配信といったサービスの提供が不可能である。

（4）サーバ側のネットワークを介して、閉域側をまたぐ不正アクセス発生の可能性がある、といった問題があり、すべての課題の解決ができない。

【0006】また、閉域網に接続しているローカルアドレスを付与されたユーザ端末がインターネット上のグローバルアドレスを付与されたサーバとの通信を行うには、ユーザ端末自身もグローバルなアドレスを持つ必要がある。しかし、前述のようにグローバルアドレスは不足するため端末にはローカルアドレスを静的に割り当てる場合が多い。この時NAT（ネットワークアドレス変換）技術により、図23に示すように閉域網内の通信はローカルアドレスを用いて行い、インターネット上のWWWサーバとの通信には、網間境界に設けたNATを利用できる装置にあらかじめプールされたグローバルなアドレスを動的に割り当てて通信を可能にする。しかし、このNATは動的にローカルアドレスとグローバルアドレスと対応つける／アドレスとポート番号の組によりホスト（端末）間の接続の識別を行うために、（1）ホストとサーバ間の接続は動的に認識されるので、一旦

10

6

接続が切断した後のローカルアドレスを静的に割り当てた端末へのグローバルアドレスを持つサーバ側からの情報配信などのプッシュ型（端末からの接続確立要求なし）のサービスは不可能、（2）サーバが各閉域網ごとの認証（識別）を行うことができないため、各所属端末毎にカスタマイズしたサービスや情報を提供することが困難、（3）NATの部分はグローバルなアドレス空間に接続しているので不正アクセスの可能性、といった問題があり、サーバ構築におけるすべての問題の解決ができない。

20

【0007】また、NAT技術自体は様々な形で拡張・利用されており、この明細書で課題としているサーバの構築に利用可能と考えられるものに、PPPと連携したNAT技術や、設定によりパケットのソースアドレスとデスティネーションアドレスの双方の変換を行えるCisco社によるNAT技術がある。PPPと連携したNATにおいては、サーバとの間にPPP接続を確立後、サーバより振り出されたグローバルIPアドレスを用いて、PPP回線を経由して外部のインターネットなどのグローバルIPネットワークとの通信においてNAT機能を行うものである。つまり確立されたPPP回線単位のNATが可能になっている。この技術を利用して課題のサーバの構築を考える。この技術をサーバ側の装置に導入すると、PPP回線毎にNATを行えるので閉域網単位で利用するサービスをカスタマイズしたり、利用するサーバを各閉域網単位で変更することが容易にできる。しかし、1台のサーバによる実現を考えると、次の問題がある。

【0008】

30

【発明が解決しようとする課題】（1）クライアントに相当するユーザの閉域網とサーバ側のネットワークがPPP接続により接続されるのでPPPトンネリング技術を利用する場合と同様に、ローカルアドレスで構築された閉域網同士の接続においてはアドレス空間の衝突が生じることになる。特に、この技術をサーバ側に導入するとクライアントに相当する閉域網のホストから到着したパケットを受けとったサーバが、閉域網のホストを示すアドレス部分の重複によりそのパケットがどの閉域網のホストから来たのかが識別できず、正しく該当するホストへパケットを送り出すことができない。

40

【0009】（2）PPP接続確立時に振りだされたアドレスに対してNATを行うので、そのアドレスに対してサーバ側の複数のサーバの持つアドレスがマッピングされるので、ユーザの閉域網のホストから複数あるサーバのうち特定のサーバへの接続を確立することができない。確立するには、利用したいサーバの数に応じてPPP回線を確立し、PPPにより取り決められるアドレスに対してサーバのアドレスを一つ対応させることが必要になる。

【0010】（3）サーバを示すアドレスに対して変換

50

7
を行うのだが、変換後のアドレスが閉域網のホストを示すアドレスと同一になると正しく通信が行えない。そのため、各閉域網のホストの利用するアドレスとサーバ側ネットワークのサーバのアドレスとが重ならないようにする必要があり、各閉域網でどのようなローカルアドレスを用いるかを調べて、サーバ側ネットワークのアドレスを決めるため多大な手間と時間がかかる。

【0011】といった問題があり解決できない、Cisco社の開発したNAT技術は、RFC1631で定義されているNATとは異なり、対象となるパケットのソースアドレスとデスティネーションアドレスの双方に対してアドレスの静的／動的な割り当てによるアドレス変換表を用いてアドレス変換が可能であり、アプリケーション層との連携、特にDNS (Domain Name System)との連携によるNATに利用するアドレス変換表を作成しての柔軟な動作が可能である。このような特徴により、従来のNAT技術では難しかったグローバルアドレスを持つインターネット上のサーバなどからNAT装置の後ろに接続されているローカルアドレスで構築された閉域網上のホストへの接続確立をも可能にしている。また、受けとったパケットの外部のホストを示すアドレスがアドレス変換表がない場合はパケットを破棄したり、または、外部のネットワークに通知するアドレスを制限するなどにより閉域網の持つ閉域性を保つこともできる。この技術を用いてこの明細書で考えるサーバの構築を行うと、(1) サーバ側ネットワークもローカルアドレスで構築された閉域網の場合、アドレス空間の衝突を避け、インターネット上のサーバなど閉域網の外のホストと通信するために双方のネットワークでNATを行う。この時、閉域網間で通信を行うにはNATに利用するグローバルアドレスとホストの持つローカルアドレスを少なくとも1対1対応にしない限り接続先のホストを特定できないため通信ができずに駄目である。この場合サーバ側から閉域網のホストへの接続ができないだけでなく、複数のサーバが存在する場合には、前述の理由により特定のサーバへの接続もできない。

【0012】といった問題がありすべてを解決できない。このように、既存の技術を用いた場合この明細書で述べているサーバ構築に生じる問題の全てを解決し得ない。

【0013】

【課題を解決するための手段】第1発明

第1発明、第2発明においてもユーザの利用している複数のユーザ側ネットワーク（以後、ユーザ側ネットワークを閉域網として説明する）はサーバ側のネットワークにPPP (Point-to-Point Protocol)による接続を行う。このPPP接続確立時の認証において従来のユーザの認証に加え、PPP接続を行ってきた接続元がどの閉域網のどのPPP回線かの認証を行う。第1発明によればその結果により、接続しているPPP接続がどの閉域

10

20

30

40

50

網のどのPPP回線かを示す情報を各PPP回線に対応付ける。そして、この情報をキーとして該当するPPP回線に割り当てられたサーバ側ネットワークのアドレスと、必要に応じて閉域網単位に決められた利用するサーバのサービスに応じたポート番号を用いて、PPP回線を通してサーバ側ネットワークに入ってくる／から出していくパケットに対してソースとデスティネーションの両方のネットワークアドレスと必要に応じてポート番号の変換を行う。

【0014】この第1発明では、サーバ側ネットワークにおいて各閉域網単位にアドレス空間を独自に割り当て、その閉域網単位の方針による柔軟な利用を行う。サーバ側ネットワークにおいて各閉域網に用意されたアドレス空間は、次の方針により割り当てる。まずPPP回線単位に静的にアドレス空間を割り当てる。このアドレス空間は、サブネット単位で割り当てるに決定する。静的な割り当て分がなくてもよい。その場合は、全て動的にサブネット単位でPPP回線に割り当てる。そして、もし残った空間があれば割り当てられたアドレス空間を消費してしまったPPP回線に対して、PPPのLCP (設定プロトコル)などを用いて動的にPPP回線に割り当てるものとする。動的に割り当てるアドレス空間の大きさは、動的にネゴシエーションにより必要分でもよいし、一定の大きさを決めておいてもよいし、あるアルゴリズムにより徐々に大きさを大きくするなど自由に選択できる。また、動的にPPP回線を割り当てる場合、どのアドレス空間をその閉域網のどのPPP回線に割り当てるかを管理しておくことで、サーバ側から閉域網側の端末へのパケットを適切なPPP回線に送り出すことができる。

【0015】このように閉域網単位で割り当てを含め動作が独立しているので、接続してくる閉域網のアドレス空間の衝突による問題の回避や、特定端末への接続を可能にしている。また、アドレスの変換はサーバ側で行われており、サーバ側で接続に関する制御が容易にでき、各閉域網の持つ閉域性を維持できるだけでなく、接続する閉域網側で、自閉域網のアドレス空間から自由に利用するサーバにアドレスを付与することが可能であり、導入時に伴うネットワークの設定変更は最小限に抑えることができる。以下、このアドレス変換方法を、ルートサイドNAT (以下、Root-side NATもしくはR NAT)と呼ぶ。

第2発明

第1発明と同様にPPP接続確立時にその回線の属するユーザの閉域網がどれかの認証を行う。そして、PPP接続確立時の所属の閉域網の認証を終了後に、PPP回線にそれがどの閉域網のどのPPP回線かを識別できるに十分なVLAN (Virtual LAN)を利用する時に利用するVLANを識別する情報を対応付ける。そして、このVLANを識別する情報をもとにスイッチング

などのV L A N構成技術により、利用するサーバへそのP P P回線よりのパケットを運ぶ。そして、1台のサーバにおいて各V L A Nを識別する情報単位に各種処理を行うOSを動作させ前述のサーバを実現する。

【0016】また、P P P回線に閉域網を識別するに十分なV L A Nを識別する情報を対応付ける場合は、パケットを受けとったP P P回線とそのパケットに示された閉域網のホストのアドレスを対応付ける。なお、この対応付けは、V L A Nを識別する情報単位に行う。これにより、ユーザのネットワークに変更を加えることなく、V L A Nを識別する情報を利用したサーバ側ネットワークの制御により容易に上述のサーバを構築、利用できる。この所属する閉域網に関する認証結果により、確立されたP P P回線に少なくとも閉域網を識別できるV L A Nを識別する情報を割り当てる方法を以下、V N A Tと呼ぶ。

【0017】

【発明の実施の形態】第1発明

まず第1発明について実施の形態を説明する。いま図1に示すシステム構成とされているとする。即ち、閉域網A、B、Cがインターネット／公衆網とそれぞれアクセスサーバA Sを介して接続され、インターネット／公衆網とサーバ側ネットワークが、この発明によるRoot-side N A T機能付きアクセスサーバR-N A Tを介して接続されている。閉域網A、Bにおいて各ホスト（端末）に対して図2 Aに示すようにアドレスが割り当てられている。つまり閉域網Aの持つアドレス空間において、ホスト1にはアドレス1、ホスト2にはアドレス2、ホスト3にはアドレス3、利用するServerにはアドレス100が割り当てられているとする。Serverはサーバ側のネットワークにおかれているホストの一つであり、このServerはサーバ側のネットワークにおいて、アドレス1が与えられている。さらに、サーバ側のネットワークにおいては図2 Bに示すように閉域網A、Bに対してそれぞれ固有のアドレス空間が用意されている。閉域網Aから接続してくる端末用にアドレス群101～300を用意しており、そのうち、ホスト1とホスト3の利用しているP P P回線1から接続してくる端末用にアドレス群101～200を、ホスト2が利用しているP P P回線2から接続してくる端末用にアドレス群201～250をそれぞれ割り当てている。そして、残りのアドレス群251～300は、前述の割り当てを使い切った場合に、P P P回線1、2に対して動的に必要に応じて割り当てる。閉域網Bの持つアドレス空間において、ホスト4にはアドレス11、ホスト5にはアドレス22、利用するServerにはアドレス150が各々割り当てられている。さらに、サーバ側のネットワークにおいては閉域網Bから接続してくる端末用にアドレス群301～350を用意しており、そのうち、アドレス群301～310までは閉域網Bの端末が直接確立するP P P回線に静的に割

り当てられている。また、311～350まではP P P回線1に割り当てられており、このP P P回線を利用するホストにサーバ接続時に動的に割り当てるものとする。このように、サーバ側のネットワークで各閉域網単位にアドレス空間をプールし、アドレス空間を閉域網の利用方針に応じてP P P回線に割り当てる、そこから更に該当するP P P回線を利用するホストへ静的、動的を含め柔軟に割り振る。

【0018】また、各閉域網におかれたアクセスサーバA SとRoot-side N A Tの機能を持つ装置R-N A Tとの間はP P P接続されている。また、閉域網の端末は、このP P P接続を利用してサーバを利用するか、P P Pトンネリングを利用して直接サーバ側におかれたRoot-side N A T機能付き装置（R-N A T）とP P P接続を行いサーバを利用する。

【0019】そこで、サーバ側のネットワーク上の物理的に1台のサーバを各閉域網にあたかも各々存在するよう仮想的に見せ、各閉域網の閉域性を失うことなく複数閉域網において利用可能にするのが、このRoot-side N A Tである。このRoot-side N A Tはサーバ側で各閉域網毎に、あらかじめ用意したアドレスを割り当てるに際し、閉域網とのP P P接続確立時に接続を要求している端末が正しいかどうかというホストに関する従来の認証だけでなく、接続してくる端末がどの閉域網のどのP P P回線に属するかの認証を行う。この結果を基に、あらかじめその閉域網のP P P回線に用意されたアドレス群の中から端末に静的にアドレスが割り振られている場合は該当するものを、そうでない場合は、P P P回線単位に用意されたアドレス空間から端末に動的にアドレスを割り振る。

【0020】図1において、ホスト1が接続してきた時、P P P回線がまだ確立していない場合、利用しているA S（アクセスサーバ）からP P P回線の確立がはじまり、この時、このP P P回線が閉域網AからのP P P回線1であることの認証を行う。そして、この閉域網AのP P P回線1用にプールされたアドレス空間からアドレスをホストに対して動的に割り当てる。今回の場合、P P P回線1には、図2 Bに示すようにアドレス空間101～200が与えられており、この空間から動的に与えるので、ホスト1には、利用されていないアドレス101をサーバ側ネットワークにおいて割り当てる。つまり、R N A Tにより閉域網AのP P P回線1よりのパケットについて閉域網Aで与えられているアドレス1がアドレス101に変換されることになる。この関係が図2 Aに示すように表として記憶される。その後、閉域網AのP P P回線1を通してホスト1からパケットが到来すると、そのアドレス1により図2 Aの表を参照してサーバ側ネットワークのアドレス101に変換される。同様に、ホスト3からのパケットが来た場合は、P P P回線1からということで同一のアドレス空間から動的にホス

ト3に、利用されていないアドレス102が割り当てられ、RNATによりホスト3の持つアドレス3がアドレス102に変換される。ホスト2がサーバに接続する場合、別のPPP回線であるPPP回線2を利用しているので、PPP回線2用に用意されたアドレス空間201-250から割り当てるうことになり、利用されていないアドレス220がサーバ側のネットワークで割り当てられ、RNATによりアドレス2がアドレス220に変換される。

【0021】ホスト4は、PPPトンネリングを利用してサーバ側の装置に直接PPP接続してきており、PPP回線の確立がはじまり、この時、同様の認証によりこのPPP回線が閉域網BからのPPP回線2であることが認証される。そして、この閉域網BのPPP回線2には静的にアドレス301が割り当てられているので、RNATによりホスト4の持つアドレス11がアドレス301にサーバ側ネットワークにおいて変換されることになる。ホスト5がサーバに接続する場合、利用するPPP回線が閉域網BのPPP回線1であることが認証され、PPP回線1に用意されたアドレス空間311-350から利用されていないアドレスが動的にホスト5に割り当てられる。今回は、アドレス311が割り当てられている。ホスト5からサーバへのパケットは、RNATによりホスト5の持つアドレス22に対してアドレス311へと変換される。

【0022】また、接続先に指定されたServerのアドレスもサーバ側のネットワークにおいてServerに割り当たったアドレスへの変換を行う。今回、閉域網Aに関してはServerのアドレス100がアドレス1に、閉域網Bに関してはServerのアドレス150がアドレス1に変換されることになる。閉域網単位に割り当たったアドレスを基にした利用するサービスの制限も可能であるが、閉域網単位に利用するサーバのポート番号を決めておくことで、サーバのポート番号により、物理的に1台のサーバにより閉域網単位のサービス提供を可能にする。今回、Serverにおいて閉域網A向けのサービスは、ポート番号Aで、閉域網B向けのサービスは、ポート番号Bで提供されているとする。

【0023】Root-side NATは、このアドレスの対応付けとポート番号を基にパケットのソースとデスティネーション両方のネットワークアドレスとポート番号の変換とをサーバ側の管理のもとで行う。実際、ホスト1がServerのWWW Server（ポート番号80）を利用する場合、ホスト1のパケットはRNATにより図3に示すような変換動作が行われることになる。図3Aはホスト1からサーバへのパケット、図3Bはサーバからホスト1へのパケットの各RNATでの変換を示す。

【0024】つまり、Root-side NATにおけるアドレス変換部分をまとめると、図4に示すようになる。この図においてNet Aは、サーバ側のネットワークのアド

レス空間においてServerが存在しているネットワークのアドレス群、Net Bはサーバ側のネットワークのアドレス空間における各閉域網用に用意されたアドレス群をまとめたものである。また、図5に示すように各閉域網用に用意されたアドレス群は、端末あるいは、ネットワークに接続している各PPP回線に静的に割り当てられ、残りの空間は、静的に割り当てられている空間が足らなくなった場合に、不足しているPPP回線に対して要求に応じて動的に割り当てるために用いる。動的に割り当てられた空間は、割り当て時にどのPPP回線に割り当てたかを管理することで、パケットを適切なPPP回線に送出することができる。このように、サーバ側ネットワークに用意された空間は、各空間の利用者である閉域網が利用の方針を選択できる。各閉域網における端末のアドレスをサーバ側において閉域網毎にあらかじめ用意されたアドレスに各々対応付けることをコンパクション（Compaction）変換、各閉域網において割り振られたServerのアドレスをサーバ側のネットワークにおけるサーバのアドレスに変換することをマージ（Merge）変換と呼ぶことにする。また、逆Compaction変換は端末に割り振られたアドレスからどの閉域網のどのPPP回線かを図2A、Bを参照して識別し、その閉域網における端末のアドレスに変換する。逆Merge変換は逆Compaction変換から得られるどの閉域網に属する端末かの情報から、サーバのアドレスを閉域網におけるサーバのアドレスに図2Aを参照して変換する。そして、どの閉域網のどのPPP回線かの識別により適切な閉域網の適切なPPP回線へとパケットを送り出す。この時、端末からサーバへのパケット、サーバから端末へのパケットのソースとデスティネーションアドレスに上記の変換を図6に示すようを行う。また、利用しているサーバのポート番号にも関してサーバ側ネットワークにおいて閉域網単位に決めたポート番号から、閉域網において利用されているポート番号へと変換する。

【0025】この各閉域網毎に与えられたアドレス空間は、所属する閉域網に関する認証の結果割り当てるところから、各アドレスがどの閉域網であるかは認証されているので、この異なる閉域網のアドレス間の接続をサーバ側で禁止することで、結果として閉域網間の通信を禁止し、閉域網の持つ閉域性を確保できることになる。さらに、各閉域網に割り当たったこのアドレス空間を基にしたり、各閉域網に対してサーバにおいて利用できるポート番号を決めて提供するサービスを閉域網毎にカスタマイズすることが可能になる。従来技術と第1発明（ルートサイドNAT）の特徴を図7にまとめて示す。

第2発明

第2発明が適用されるシステム構成を図8に示す。閉域網A、BがそれぞれアクセスサーバA5を介してインターネット／公衆網と接続され、またサーバ側ネットワー

13

クがV NAT機能付きアクセスサーバV NATを介してインターネット／公衆網と接続されている。V NAT機能付きアクセスサーバV NATでは図9に示すようにV LANタグを各閉域網の各PPP回線に割り当てる。以下、この割り当てによる変更をV NATと呼ぶ。各閉域網におかれたアクセスサーバASは、サーバ側ネットワークにあるV NAT機能を持つアクセスサーバV NATにPPP接続を行う。

【0026】ホスト1, 2, 3は、いずれも閉域網Aのホストであることから、閉域網Aを示すV LANを利用する時に利用するV LANを識別する情報、例えばV LANタグとしてV LAN1-xが割り当てられる。次に、同一閉域網からの複数のPPP回線を識別するために子番号xを割り当てる。ホスト1と3は、同一のPPP回線1から来ており、V LANタグとしてV LAN1-1がPPP回線1と対応付けされている。また、ホスト2は、閉域網AのPPP回線2を利用して接続していることから、V LANタグとしてV LAN1-2が該当するPPP回線2に対応付けられている。同様に、ホスト4, 5は閉域網Bに属するホストであることから、閉域網Bを示すV LANタグとしてV LAN2-xが割り当てられることになる。閉域網Aの場合と同様にPPP回線を識別するために、ホスト4にはV LAN2-2がホスト5にはV LAN2-1が割り当てられる。

【0027】図10に示すようにV NAT機能を持つ装置V NATにおいてV LANタグの割り当てに基づき閉域網から受け取ったパケットにこのV LANタグを埋め込む。そして、このパケットは、IEEE802.10やV LAN対応のスイッチング機能などの既存のV LAN技術によりServerまでこのV LANタグに基づき運ばれる。パケットを受け取るServerは、図11に示すようにV LANタグ毎に別々の処理を行うために複数のOSが動作できるように変更し、閉域網を識別できる単位のV LANタグに対し1つのOSが動作するようとする。つまり、V LAN1-xのタグに関する処理を行うためのOS1, V LAN2-xのタグに関する処理を行うためのOS2をという具合に1台のマシンの中で複数のOSを動作させることになる。サーバ側のネットワークにおいては、V LANタグを基にパケットの配達が行われるのでサーバ側のネットワーク上のサーバを含めて仮想的な閉域網を構築することができるので、パケットのアドレスに関してサーバ側では何ら変換を行う必要はない。このように、1台のサーバにおいてV LANタグ毎にOSを動作させることでサーバ側の管理の下、閉域網の持つ閉域性を失うことなく仮想プライベートサーバを構築できる。

第2発明の変形

第2発明の変形例を以下に示す。ホスト1, 2, 3はいずれも閉域網Aのホストであることから、閉域網Aを示すV LANタグとしてV LAN1が割り当てられる。次

10

に、同一閉域網からの複数のPPP回線が確立された場合に、パケットを受けとったPPP回線へとそのホスト宛のパケットを送り返すことができるよう、ホストを示すアドレスとPPP回線を対応付ける。ホスト1と3は、同一のPPP回線1から来ており、各々のアドレスがPPP回線1へ対応付けられる。また、ホスト2は、閉域網AのPPP回線2を利用して接続していることから、V LANタグとしてはV LAN1が割り当てられるが、ホスト2のアドレス2がPPP回線2に対応付けされる。

20

【0028】同様に、ホスト4, 5は閉域網Bに属するホストであることから、閉域網Bを示すV LANタグとしてV LAN2が割り当てられることになる。閉域網Aの場合と同様に受けとったPPP回線にパケットを送り返すためにホストのアドレスとPPP回線とを対応付ける。この場合、ホスト4のアドレスがPPP回線2へ、ホスト5のアドレスがPPP回線1に対応付けられる。図12に示すようにこのPPP回線とホストのアドレスの対応付けはV LANタグ単位に行うので、V LAN1, V LAN2の各々独立して対応付けが行われる。参考までに、V LAN1に関する対応付けは以下のようなものとなる。この対応付けにおいて最新の接続時刻も合わせて管理して、タイムアウトを設けるなどによりセキュリティを高めることも出来る。サーバからのパケットを受けとるとこのV NAT変換を行っている装置において、パケットに埋め込まれているV LANタグをキーとして、まず検索する対応表を決め、次にパケットに埋め込まれているデスティネーションアドレス（ホストのアドレス）をキーとして対応表を検索し、送り出すべきPPP回線を調べる。その結果により、パケットを受けとったPPP回線へと送出することができる。

具体例

この発明の方法により可能となる仮想プライベートサーバを利用した具体例として、複数業者を対象とする調達業務の例を用いて述べる。今回、企業1が調達のために各々企業A, Bに調達依頼をし、どちらか良い方を選択するために企業間でデータの登録、交換しあうことが必要となる場合での具体例である。

第1発明の具体例

図13に示すようなネットワーク構成になっているとする。閉域網A, B, 1はそれぞれアクセスサーバAS1, AS2, AS3によりインターネットと接続され、ISDN網がアクセスサーバAS4によりインターネットと接続され、サーバ側ネットワークがルートサイドNAT機能付きアクセスサーバR-NATによりインターネットと接続されている。また、ルートサイドNAT機能を持つ装置R-NATにおいては図14に示すようにアドレスの変換表を作成して動作する。変換表の作り方は後述する。ここで、閉域網Nは、企業Nの持つ閉域網を意味するものとする。サーバ網のネットワークにおか

50

15

れたルートサイドNAT機能付き装置R-NATと各閉域網に置かれたアクセスサーバAS1, AS2, AS3との間はトンネリングを利用してPPP接続される。また、ISDNなどをを利用してアクセスサーバAS4に接続し、これを経由して閉域網に属するホストが直接サーバ側ネットワークにある装置R-NATとPPP接続を行うこともできる。

【0029】各閉域網のホストには所属する閉域網の持つアドレス空間から図12に示すようにアドレスが各々割り振られている。このRoot-side NATの機能を利用するため、サーバ側のネットワークにおいて各閉域網のためにアドレス空間をプールしてある。この例において、閉域網Aにはエアアドレスで表わして10.10.1.0サブネットマスク255.255.255.0のアドレス空間を用意し、この空間から閉域網Aから接続してくる端末にアドレスを割り当てる。同様に、閉域網Bには10.10.2.0サブネットマスク255.255.255.0のアドレス空間を用意し、この空間から閉域網Bから接続してくる端末に、閉域網1には10.10.11.0サブネットマスク255.255.255.0のアドレス空間を用意し、この空間から閉域網1から接続してくる端末にアドレスを割り当てる。

【0030】閉域網Aにおいて、ホスト1は10.0.1.13、ホスト2は10.0.3.20、利用するWWW Serverに10.1.1.1が割り当てられているとする。実際には、WWW Serverはサーバー側のネットワークにおいて、このWWW Serverはサーバー側のネットワークにおいて、10.100.10.1が割り当てられ、異なる複数の閉域網に属する端末に対してサービスを提供している。サーバ側のネットワークにおいて閉域網Aに割り当てられているアドレス空間10.10.1.0サブネットマスク255.255.255.0のうち、10.10.1.0サブネットマスク255.255.255.192はPPP回線1に、10.10.1.64サブネットマスク255.255.255.192は、PPP回線2に割り当てられている。そして、残りの空間10.10.1.128サブネットマスク255.255.255.128は動的にPPP回線1, 2からの要求に応じてサブネットワーク単位で要求してきたPPP回線に割り当てるためにとつてある。また、閉域網Aの端末がWWW Serverを利用する場合、サーバ側のネットワークにおいて、ポート番号8080番で閉域網A用のサービスを展開するように設定されている。

【0031】今、ホスト1がWWW Serverを利用する場合、アクセスサーバ1(以下、AS1)から確立されるPPP回線1を利用するようになっている。もし、AS1とサーバ側のRoot-side NAT機能付きAS(以下、RNAT装置)との間にPPP回線1が確立していない場合、まずPPP接続を確立する。この時、ホスト

10

20

30

40

16

の認証だけでなくどの閉域網のどのPPP回線かを認証する。この場合、閉域網AのPPP回線1であることが認証される。次に、閉域網AのPPP回線1用にサーバ側ネットワークにおいて割り当てられているアドレス空間に利用していないアドレスがあるかをチェックする。今回の場合は使用されていないアドレスがあるとし、その空間からホスト1に動的に10.10.1.15が割り当たられる。もし、すでにPPP回線1用の空間がすべて使用されている場合、AS1がPPPのLCPなどを利用して必要な分のアドレス空間を要求し、これに応じてRNAT装置において、閉域網Aの持つ動的に割り当てるために用意されている空間10.10.1.128サブネットマスク255.255.255.128から要求のうち許可分を新たに複数のPPP回線1に割り当てる、その中から動的にホスト1にアドレスを割り当てる事になる。この時、割り当てる空間がどのPPP回線に割り当てたかをRNAT装置で管理し、これによりパケットを適切なPPP回線へと送り出せる。動的に割り当てるのは、サブネット単位の要求分を割り当てる他に、決まった一定のサブネット空間分でもよいし、徐々にサブネット空間を単位として大きくしていくてもよい。

【0032】ホスト2は、閉域網Aにおいてアドレスが10.0.0.3.20であり、AS1とRNAT装置間に確立されるPPP回線2を利用してサーバに接続する。ホスト1が接続する場合と同様に、このPPP接続確立時にこのPPP回線が閉域網Aに属するPPP回線2であることが認証される。そして、閉域網AのPPP回線2用に用意された空間10.10.1.64サブネットマスク255.255.255.192から使用されていないアドレスを検索し、ホスト2に割り当てる。今回、ホスト2には、10.10.1.100が動的に割り当たる。もし、あらかじめ用意された空間がすべて使用されていたら、ホスト1の時と同様にして動的にアドレス空間をPPP回線2に割り当てる、その空間から動的にホスト2に割り当てる。このようにして、接続してきたホストにサーバ側のネットワークにおいてアドレスが割り当てられ、RNAT機能に必要なアドレス変換表が作られる。

【0033】ホスト1からWWW Serverへの場合、RNAT装置においてパケットのソースアドレスを10.0.1.13から10.10.1.15へ、デスティネーションアドレスを10.1.1.1から10.10.10.1へと変換する。また、WWW Serverを利用するため、サーバのポート番号80にホスト1は利用要求を出すが、RNAT装置において閉域網A用のサービスを提供しているサーバのポート番号8080にポート番号も変更して、変換後サーバ側ネットワークのルーティングにより正しくサーバに送られ、閉域網A向けのサービスの利用が行われる。

50

【0034】逆にWWW Server からホスト1へのパケットは、デスティネーションアドレスを10. 10.

1. 15から閉域網Aに属するホスト1であることとAS1から確立されているPPP回線1向けのパケットであることを識別し、アドレスを10. 0. 1. 13へと変換する。次にホスト1が閉域網Aに属しているという情報からソースアドレスを10. 100. 10. 1から10. 1. 1. 1へ変換する。そして、ポート番号も8080からホストが送ってきたパケットに指定されていたポート番号80へと変換される。この変換後、受け取ったパケットの持つデスティネーションアドレスに基づく情報により適切なPPP回線である閉域網AのPPP回線1へパケットを送り出す。

【0035】同様に、閉域網Bの場合について述べる。閉域網Bにおいて、ホスト3は10. 0. 1. 30、ホスト4は10. 0. 1. 14、利用するWWW Serverに10. 10. 15. 1を割り当てているとする。実際には、WWW Serverはサーバ側のネットワークにおいて、このWWW Serverは前述同様、サーバ側のネットワークにおいて、10. 100. 10. 1が割り当てられている。サーバ側のネットワークにおいて、閉域網Bに割り当てられているアドレス空間は、10. 10. 2. 0サブネットマスク255. 255. 255. 0であり、閉域網Bでは、端末自身がR NAT装置に直接PPP接続する利用も行われており、そのため、10. 10. 2. 64. サブネットマスク255. 255. 255. 192の空間をそれらのために用意し、各PPP回線と1対1対応にアドレスを静的に割り振っている。今回、PPP回線2以降が端末から直接確立されるPPP回線とし、PPP回線2には、10. 10.

2. 65が割り当てられており、他の該当するPPP回線もアドレスが1つ静的に割り当てられている。また、AS2から確立されるPPP回線1用には10. 10. 2. 0サブネットマスク255. 255. 255. 192の空間を静的に割り当てており、このPPP回線を利用するホストにアドレスはこの空間から動的に割り当られる。残りの空間10. 10. 2. 128サブネットマスク255. 255. 255. 128は割り当て分を使用したPPP回線1からの要求に応じて動的に割り当てるために用意してある。

【0036】ホスト3はAS2により確立されているPPP回線1を利用して接続しているので、閉域網Aのホスト1や2の場合と同様に、利用しているPPP回線が閉域網BのPPP回線1であることが認証されると、静的に割り当てられた空間10. 10. 2. 0サブネットマスク255. 255. 255. 192に使用されていないアドレスがあるかを検索し、あればその中から任意のものを割り振る。今回、ホスト3にはサーバ側ネットワークにおいて、10. 10. 2. 10が割り当てられる。ホスト4は、今、移動しており最寄りのAS4に着

呼び、PPPトンネリングを利用してR NAT装置に対して直接PPP回線を確立する。この確立時に、PPP回線が閉域網BのPPP回線2であることが認証され、PPP回線2は静的にアドレスが1つ割り当てられており、この例では割り当てられているアドレス10. 10. 2. 65がホスト4のアドレスとなる。また、WWW Serverのアドレスは閉域網Aの場合と同じである。また、利用するサービスを示すポート番号は、閉域網Bにはポート番号8081が割り当てられている。

【0037】実際のホストからWWW Server（ポート番号80）への通信時には、ホスト1, 2の場合と同様に図14に示す変換表などによりR NAT装置において、パケットの持つソースとデスティネーションアドレスを各々変換し、さらにポート番号に関して、80から閉域網Bに対して指定されている8081番に変換される。逆にWWW Serverからホストへのパケットも、前述と同様にパケットの持つソースとデスティネーション双方のアドレスとポート番号を変換する。この変換時に、パケットのデスティネーションアドレスによりホストの所属する閉域網がどれであるか、その閉域網から複数のPPP回線が存在する場合には、どのPPP回線へ送り出すかを判断できる。また、この情報を基にサーバに対して接続しているポート番号も変換される。そして、アドレスとポート番号が変換後、適切なPPP回線へと送出される。例えば、ホスト3へのパケットの場合は、10. 10. 2. 10がデスティネーションアドレスとして与えられているので、これにより閉域網BのPPP回線1へ送り出せば良いパケットであることが識別されて送り出される。

【0038】閉域網1のホスト5の場合も同様に動作し、閉域網1の決めたアドレス空間の割り当て方針によりアドレスがホスト5に割り当てられ、図13に示すような表が作られ、これをを利用してアドレス変換がホスト5に関して行われる。また、閉域網1用に決められたサーバ利用時のポート番号8088とすると、ポート番号に関しても変換が行われる。サーバ側ネットワークからホストへのパケットに対しても前述と同様の仕組みにより適切な閉域網の適切なPPP回線へと送られる。

【0039】ここで、アドレスは所属する閉域網を認証した結果としてサーバ側のネットワークにおいて割り振られるので閉域網を示すという意味においてアドレスは保証されていることになり、このアドレスを基に制限を行うことは、閉域網単位での制限を行ことと同等である。つまり、アドレス10. 100. 10. 1を持つWWW Serverは、10. 10. 1. 0サブネットマスク255. 255. 255. 0、10. 10. 2. 0サブネットマスク255. 255. 255. 0、10. 11. 0サブネットマスク255. 255. 255. 0の各アドレス空間からの接続のみを許可することで、これ以外のアドレス、つまり他の閉域網からの利用

19

を容易に制限ができる。これにより、限られた閉域網間での通信を閉域性を保ちながらできる。また、アドレスを利用したデータへのアクセス制限だけでなく、今回のように閉域網単位で利用するポート番号を決めておき、そのポート番号単位にそれに応答するプログラムを動作させ、参照できるデータ、参照して変更できるデータなどを設定しておくことで物理的に一台のサーバによる複数閉域網向けにカスタマイズしたサービスが実現できる。

【0040】今回の場合、閉域網A、Bに割り当てているポート番号8080と8081に対して動作しているプログラムがアクセス、操作できるデータを各々区別することで、同一サーバ上にデータがあつても閉域網Aは自分の登録したデータは参照・変更はできるが、閉域網Bの登録したデータは変更する事はもちろん見ることもできないようになる。逆に、閉域網1に割り当てたポート番号8088に対して動作しているプログラムは、先のポート番号8080と8081で動作しているプログラムがそれぞれアクセス、操作できるデータの両方にアクセスすることが出来るようにすれば、閉域網1のホストは、閉域網A、B双方が独立して管理するデータを参照できる。これにより、今回の例としている調達業務において要求される注文主の企業1が注文先である企業A、B双方のデータを自由に見ることが出来るという課題がクリアされる。これは、今回のようにポート番号で制限を行ってもよいし、閉域網単位に割り当てたアドレス空間を用いて制限を行っても良い。また、異なるアドレス空間における通信を禁止することで、サーバ側のネットワークを介した異なる閉域網間での通信を防止でき、閉域網の持つ閉域性を維持することができる。さらには、接続先のサーバのアドレスもサーバ側で管理できるので、複数のサーバを用意しておけばサーバの負荷に応じてアドレスの変換を行うことでサーバの負荷分散也可能になる。

【0041】次に、IPネットワークによる通信時に重要な働きをするDNS(Domain Name System)サーバとの動きを、閉域網Aとサーバ側ネットワークとの通信時を例として述べる。図12において、まずユーザの閉域網に属するホストがサーバ側のネットワークのホストに接続する場合を述べる。閉域網Aに属するホスト1がサーバ側ネットワークのWWWサーバに接続するために、閉域網A上のDNSサーバ2に接続したいWWWサーバのアドレスを問い合わせる。閉域網Aのアドレス空間においてWWWサーバに対してアドレスが割り当てられているので、DNSサーバ2は閉域網Aで該当するサーバに割り当てられたアドレス10.1.1.1をホスト1に返す。そして、ホスト1は、ソースアドレスを自分の持つアドレス10.0.1.13、デスティネーションアドレスをサーバの持つアドレス10.1.1.1、デスティネーションのポート番号80としたパケットを送

50
20
出する。そして、閉域網Aのネットワークにおいて10.1.1.1宛のパケットをAS1へ届くように正しくルーティングを設定しておくことで、このパケットは、AS1に届き、必要ならばPPP回線を確立してサーバ側ネットワークのRNAT機能付き装置まで運ばれる。このパケットを受け取ったRNAT機能付き装置はパケットのデスティネーションアドレスを自身の持つ変換表を基に、10.1.1.1から10.100.10.1へと変換する。次に、ソースアドレスの10.

0.1.13を変換表の中において検索する。検索した結果、該当するアドレスが存在するとそのアドレスを利用して、今回の例の場合は10.10.1.15に変換し、さらにデスティネーションのポート番号80を、閉域網A用に割り当てられたポート番号8080に変換され、そのパケットは該当するサーバへと運ばれる。もし、該当するアドレスがない場合は前述の方法によりサーバ側ネットワークにおいて割り当てられ、以下通常の場合と同様に通信が行われる。

【0042】もし、仮にDNSサーバ2に接続したいサーバのアドレスが登録されていない場合、DNSサーバ2はサーバ側ネットワークのDNSサーバであるDNSサーバ1にサーバのアドレスを問い合わせる。この問い合わせパケットはルーティングによりAS1を経由してサーバ側ネットワークのRNAT装置に送られる。受け取ったRNAT装置は、パケットのソースとデスティネーションアドレスの両方を変換表に基づき変換する。そして、該当パケットがDNSのアドレス問い合わせパケットの場合、パケットのデータには変更を加えずDNSサーバ1へ送る。DNSサーバ1は、指定された接続先のサーバのアドレスをレスポンスとして返す。今回の場合、サーバのアドレス10.100.10.1がデータとして埋め込まれる。このレスポンスパケットは、サーバ側ネットワークのルーティングによりRNAT装置へと送られる。受け取ったRNAT装置はデスティネーションアドレス10.10.1.62(サーバ側ネットワークにおいて閉域網AのDNSサーバ1に静的に割り当てたアドレス)からパケットが閉域網AのAS1から来ているPPP回線1に送り出せばよいことを識別し、閉域網Aに関する変換により正しくソースとデスティネーションアドレスを変換する。また、このパケットがDNSのレスポンスパケットでありホストのアドレスを返すものである場合、データとして埋め込まれたサーバのアドレス10.100.10.1を閉域網Aにおいて割り当てられたサーバのアドレスである10.1.1.1に変換され、このパケットはDNSサーバ2へと送られる。これを受け取ったDNSサーバ2は、10.1.1.1を接続したいサーバのアドレスとしてホスト1へ答え、ホスト1は通常の接続と同様にパケットを送出し通信を行う。

【0043】逆にサーバ側ネットワーク上のWWWサー

21

バが閉域網のホスト1に接続する場合について述べる。まず、サーバ側ネットワークのサーバがホスト1のアドレスをDNSサーバ1に問い合わせる。DNSサーバ1はホスト1のアドレスを知らないので、ホスト1の名前に含まれているドメイン名などからホスト1がまず閉域網Aに属するホストであることを認識する。そして、閉域網AのDNSサーバであるDNSサーバ2に対してサーバ側ネットワークで割り当てたアドレス(今回の場合、10.10.1.62)をデスティネーションアドレスとしてアドレス問い合わせのパケットを送出する。このパケットはサーバ側のネットワークにおいてR NAT装置へとルーティングされる。パケットを受け取ったR NAT装置はデスティネーションアドレスから閉域網AのPPP回線1向けのパケットであることを識別し、閉域網Aのアドレス空間へとソースとデスティネーションアドレスの両方を自身の持つ変換表により変換する。そして、閉域網AのDNSサーバ2へと送出される。

【0044】このパケットを受け取ったDNSサーバ2は、問い合わせられているホスト1の閉域網Aでのアドレス10.0.1.13をレスポンスとして、サーバ側ネットワークのDNSサーバ1へと送る。このパケットはサーバ側ネットワークのR NAT装置が受け取り、まずソースとデスティネーションアドレスを各々変換表より変換する。そして、このパケットがホストのアドレス問い合わせの答えであることからデータに埋め込まれているホストのアドレス部分をサーバ側ネットワークのアドレスへと変換する。この時、R NAT装置の持つ変換表を検索し該当するデータがあれば、変換表から対応するアドレスへと変換して、DNSサーバ1へ送る。また、該当するデータがない場合は、前述の方法によりホスト1へ閉域網AのPPP回線1用に割り当てたアドレス空間から動的にアドレスを割り当て、割り当てたアドレスへDNSサーバ2からのレスポンスであるホスト1のアドレスを変更し、DNSサーバ1へ送る。今回は、アドレス10.10.1.15が割り当てられ変換されることになる。この時、R NAT装置の持つ変換表に該当するホスト1に関するアドレスデータを付加する。このようにDNSサーバのレスポンスであるホストのアドレスは変換され、変換されたアドレスが該当する閉域網のホストに接続要求しているサーバへと通知される。そして、通知されたアドレスをデスティネーションアドレスとして、サーバは閉域網に属するホストへの接続を試み、R NATによるアドレス変換機能によりサーバ側からホストへの接続が確立されて通信が開始される。

【0045】このようにすることでDNSサーバとの連携が可能であり、既存のDNSサーバに変更を加える必要がなく利用が可能となり、多くの通信に利用されているIPネットワークでの導入が容易であり、またサーバと閉域網のホストの双方向からの接続の確立が実現できる。また、DNSサーバを利用してアドレスの通知を制

10

30

40

22

限すればサーバからの接続ができる閉域網のホストを限定するなど細かな制御も出来、閉域網の方針による閉域性の維持ができる。

【0046】以上から、サーバ側のネットワークにおいて各閉域網毎にアドレス空間を用意し、さらには、各閉域網ごとにサーバに対して利用できるポート番号を決めて、受けとった／送り出すパケットの該当する各部分を変換しているので、サーバ側から端末への情報配信や閉域網毎、あるいは、地域毎にカスタマイズしたサービスの実現が可能になる。さらに閉域網単位にアドレスを割り当てるので閉域網の持つ閉域性を保持したまま複数閉域網に対し1台のサーバによるサービスの提供ができる仮想プライベートサーバの構築を可能にする。また、動的に割り当てるアドレスの割り当て有効期限をある一定時間／あるイベント終了までとすることで、一度動的に割り当てるアドレスの再利用が可能でありスケーラビリティやセキュリティを確保することも可能である。

第2発明の具体例

第1発明の具体例の場合と同様に、企業1が企業A、Bに対して調達を行う場合を例にして述べる。ネットワークの構成は、図15に示すようなものとなっている。即ち閉域網A、B、1はそれぞれアクセスサーバAS1、AS2、AS3によりインターネットと接続されサーバ側ネットワークはVNAT機能付きアクセスサーバによりインターネットと接続されている。閉域網Nは、企業Nの持つ閉域網を示している。また、VNAT機能を持つ装置においては図16に基づき各閉域網のPPP回線単位にVLANタグを割り当てる。ホスト1がサーバ側ネットワーク上のサーバを利用する時、AS1とVNAT機能付AS(以下、VNAT装置)との間にPPP接続がなければPPP接続を確立する。このPPP接続確立時の認証において、このPPP回線が閉域網AのPPP回線1であることが認証される。閉域網Aを示すVNATタグとしてVLAN1が割り当てられており、これまでPPP回線1を示すために子番号を用いてこのPPP回線1に対してVNAT1-1というVLANタグが割り当たられる。これにより、閉域網AのPPP回線1であることを識別できる。PPP回線2が確立した場合は、VLAN1-2というように子番号をPPP回線に対応させるものとする。VLANタグの形式は既存のVLAN技術を利用するため、IEEE802.1Qなどで定義されているものなど既存のものを用い、情報量としてここに述べたどの閉域網のどのPPP回線であるか識別できるものであればよい。

【0047】VNAT機能によりこのPPP回線を通してサーバ側のネットワークに来るパケットに関しては、図9に示したようにVLANタグを埋め込み、このタグを基にサーバへ配達される。そして、サーバではVLANタグ毎に様々な処理を行うプログラム、例えばOSを別個に動作させ処理を行う。このサーバではVLANタ

グと接続してきたホストの情報を関連付けることでホストへ向けてパケットの送出時には、適切なVLANタグをつけて送り出すことができる。これにより、サーバ側ネットワークでのアドレスの変換は必要とすることなく、自閉域網に存在するかのようにサーバを利用できる。また、VLANタグ毎にOSが動作しているためにその動作は閉域網単位で柔軟に変更できるようになっており、参照・登録するデータもVLANタグをキーにして制限をかけることができる。サーバ側ネットワークから閉域網へ送り出される時には、受け取ったパケットについているVLANタグを取り除き、VLANタグからパケットの配送先として適切な閉域網と適切なPPP回線を識別し正しいPPP回線へと送り出す。

【0048】ホスト2がサーバ側のネットワークに接続する場合は、PPP回線2を利用するので、このホスト2からサーバ側ネットワークへのパケットには前述の方法と同様にVLANタグが割り当てられVLAN1-2を用いることになる。このタグを用いて、ホスト1の場合と同様に動作する。各々のパケットに埋め込まれるVLANタグは異なるが、サーバは閉域網Aを示すVLAN1を基にして動作を決定するので、利用するPPP回線が異なっていても同一のデータを参照・変更できる。逆に、サーバからホスト1, 2へのパケットはVLANタグにより閉域網Aへのものであることが識別され、さらにVLANタグの子番号を基にホスト1へのパケットはPPP回線1へ、ホスト2へのパケットはPPP回線2へと適切に振り分けられる。

【0049】ホスト3, 4は同じAS2を介してサーバ側ネットワークに接続しており、ともにPPP回線1を利用しているので、利用するVLANタグは同じでVLAN2-1を用いて、VNAT装置においてパケットに組み込まれ、サーバへと送られる。サーバからホストへのパケットも前述のホスト1と同様にして適切なPPP回線を通りホストへと送られる。

【0050】ホスト5の場合も同様に、PPP接続確立時に所属する閉域網が閉域網1であり、これがPPP回線1であることが認証され、それに基づき閉域網1を示すVLANタグであるVLAN3、PPP回線1を示すVLANタグであるVLAN3-1が割り当てられる。そして、他のホスト同様の動作により正しくホストとサーバ間においてやり取りされる。また、VLANタグがVLAN3に関する処理をするOSからは、VLANタグがVLAN1, VLAN2しか参照できないデータを参照することができるようになることで、企業1のユーザは、企業A, Bが登録したデータを見ることができ、今回の例となっている調達業務に必要となる制限付きの閉域網間の通信が実現される。

【0051】次に、IPネットワークによる通信時に重要な動きをするDNS(Domain Name System)サーバとの動きであるが、第2発明の場合はサーバは確かにサー

バ側のネットワーク上にあるが、VLAN機能の利用により仮想的に閉域網内での通信が実現されているので、DNSサーバは通常の場合と同様の利用が可能であり、サーバに割り当てられたアドレス宛のパケットが正しく閉域網においてサーバ側のネットワークにあるVNAT装置とPPP接続できるASへと正しくルーティングされるように設定するだけで利用が可能になる。

【0052】このようにして、サーバのアドレスをデステイネーションアドレスとし、そのパケットがサーバ側ネットワークへ運ばれるようになると、ユーザ側のネットワークに変更を最小限にしてサーバ側の制御のもと1台のサーバにより複数の閉域網に対して各々サーバがあるかのように動作できる仮想プライベートサーバによるサービスの提供が可能になる。

【0053】第2発明の変形に対する具体例を以下に示す。PPP回線確立時に所属する閉域網の認証を行い、閉域網単位で、PPP回線と受けとったパケットの送出元であるホストのアドレスとを対応付ける。今回の場合、図17に示すような表をVNAT装置が持つことになる。また各閉域網A, B…に対してVLANタグ、VLAN1, VLAN2, …が予め割り当てられてある。

【0054】ホスト1がサーバ側ネットワークに接続を試みると、AS1とVNAT装置との間にPPP回線1が確立され、閉域網Aであることが認証される。そして、この認証結果によりVLANタグのVLAN1がこのPPP回線1に割り当てられる。そして、ホスト1からのパケットがVNAT装置に到着すると、VNAT装置ではパケットに埋め込まれたホスト1のアドレス10.0.1.13と、パケットが運ばれてきたPPP回線1とを対応付ける。そして、認証結果により割り当てられたVLANタグを埋め込み、サーバへと送られる。逆に、サーバからパケットが到着すると、埋め込まれたVLANタグのVLAN1により図17の対応表からVLAN1に関するものを選択し、パケットのデスティネーションアドレスであるホスト1のアドレス10.0.1.13をキーにして検索を行い、対応表よりこのパケットを閉域網Aとの間に確立されたPPP回線1に送り出せばよいことを認識し、VLANタグを取り除きPPP回線1へと送り出す。このようにして、同一の閉域網から複数のPPP回線が確立された場合でも、パケットを受けとったPPP回線へ正しくパケットを送り出すことができる。

【0055】ホスト2の場合は、閉域網Aに属するホストであるので、ホスト1と同様にVLAN1が割り当てられる。しかし、利用しているPPP回線がホスト1と異なるので、ホスト2のアドレス10.0.3.20はPPP回線2へと対応付けられる。これにより、ホスト1と同様にVLAN1がパケットに埋め込まれるが、サーバからのパケットはこの対応表により、ホスト2宛のパケットは適切にPPP回線2を利用して送られる。ホ

25

スト3、4、5の場合も同様の方法によりVLANタグが割り当てられ、ホストのアドレスとPPP回線が割り当てられ、VLANタグ単位で独立して管理される。これにより、適切な閉域網の適切なPPP回線へとパケットを送り出すことができる。

【0056】次に図18を参照して図1中のR-NAT装置、つまりルートサイドNAT機能付きアクセスサーバの概略機能構成を説明する。複数のPPP回線処理部11が設けられPPP回線確立部11には認証部12が付属されている。PPP回線確立の際にどの閉域網のどのPPP回線であるかの認証が認証部12で確認され、図2Bに示したアドレス割り当てテーブル13を参照してそのPPP回線を利用して到着したパケットのホストにサーバ側ネットワークの割り当て分のうち空きアドレスが割り当てられ、その各閉域網のPPP回線と閉域網側のアドレスと、割り当てたサーバ側ネットワークのアドレスとの対応表(変換表)14が作られる。PPP回線処理部11に端末からパケットが来ると、そのPPP回線が確立していれば、その閉域網とPPP回線に該当する対応表14を参照して、そのパケットのアドレスに対して、アドレス変換部15でアドレス変換を行ってサーバ側ネットワークへ送られる。サーバ側ネットワークからのパケットは、そのアドレスにより対応表14を参照して、閉域網側で付与したアドレスに変換すると共にどの閉域網のどのPPP回線かを知り、対応するPPP回線処理部11よりPPP回線へ送出する。

【0057】このR-NAT装置において閉域網からパケットに対する処理は図19に示すようになる。まず最初のパケットの到来に先立ち、PPP回線接続要求があるかがPPP回線処理部11で調べられ(S1)、接続要求であればどの閉域網のどのPPP回線からの要求であるかを認証し(S2)、PPP回線を確立する(S3)。

【0058】この状態でそのPPP回線を利用したホストからのパケットを待ち(S4)、パケットが到来すると、その閉域網とソースアドレスにより対応表14を検索し(S5)、対応するものがなければ、そのパケットのアドレスに対し、アドレス割り当てテーブル13を参照してサーバ側ネットワークのアドレスを割り当て、これらの関係を対応表14に書込む(S6)。到来パケットについてそのアドレスで対応表14を検索し、アドレス変換部15でアドレス変換してサーバ側ネットワークへ送る(S7)。その後に到来するパケットはPPP回線が確立されているから、ステップS4のパケット待ち状態にあり、また対応表14の検索によりアドレスが見つかる場合は(S5)、対応表(変換表)14にもとづくアドレス変換を行ってサーバ側ネットワークへ送出する(S7)。見つからない場合は、上記のようにアドレス割り当て対応表14を作成する。

【0059】次に図8中のVNAT装置(VNAT機能

10

20

30

40

26

付きアクセスサーバ)の概略機能構成を図20を参照して説明する。図18の場合と同様に複数のPPP回線確立部11、これに付属する認証部12が設けられ、PPP回線確立時に、どの閉域網のどのPPP回線かが認識され、そのPPP回線には図9に示すようなVLANタグテーブル21によりその閉域網のそのPPP回線と対応したVLANタグが割り当てられる。そのPPP回線を通じて到来したパケットに対し、パケット変換部22で、そのPPP回線に割り当てられたVLANタグが附加されて、サーバ側ネットワークへ送出される。

【0060】サーバ側ネットワークから到来したパケットは、パケット変換部22でそのVLANタグによりVLANタグテーブル21を検索し、対応するPPP回線へ、VLANタグを除去して送出する。このVNAT装置における閉域網からのパケットに対する処理は図21に示すようになる。まず最初のパケットの到来に先立ち、PPP回線接続要求があり(S1)、どの閉域網のどのPPP回線からの要求であるかの認証を行い(S2)、PPP回線を確立する(S3)。

【0061】その後、その確立したPPP回線にパケットが到来すると(S4)、その閉域網のそのPPP回線でVLANタグテーブル21を検索して該当するVLANタグを取り出し(S5)、これをパケット変換部22でパケットに埋込みサーバ側ネットワークへ送る(S6)。VLANタグとして、PPP回線を区別する番号を用いない、図12や図17を参照して説明した場合においてはVNAT装置は図20中のVLANタグテーブル21が閉域網とVLANタグとの対応を示すものとなり、更に図20中に破線で示すようにPPP回線が確立され、埋込むVLANタグが決まると、図12又は図17に示すような、そのVLANタグとそのPPP回線と、そのパケットの閉域網の(ソース)アドレスとの関係を示す対応表23を作成する。サーバ側ネットワークからのパケットは、そのVLANタグと、その(デスティネーション)アドレスとにより対応表23を参照してパケット変換部22でどの閉域網のどのPPP回線へ、VLANタグを除去したパケットを送るかを決定する。

【0062】図21に示した処理においては、ステップS6の代りに破線で示すようにVLANタグを埋込み送出すると共にVLANタグと、到来したPPP回線と(ソース)アドレスとの対応表を作成することになり、その他は同様である。上述では複数閉域網間の通信にこの発明を適用したが、複数ユーザ側ネットワークとサーバ側ネットワークとの通信にもこの発明は適用できる。

【0063】

【発明の効果】この発明では、PPP接続により各閉域網がサーバ側のネットワークに接続され、このPPP接続確立時に所属する閉域網とPPP回線自体を認証することにより、閉域網単位に割り当てたアドレス空間により様々な制御がサーバ側で容易に行える。これにより、

50

27

複数の閉域網のユーザ端末に対し、閉域性を失うことなく各閉域網にカスタマイズした共通サービスの提供を物理的に1台のサーバにより可能にし、各閉域網からは自閉域網に各々サーバが存在するように利用できる。また、今後増えゆくと予想される複数企業間でのデータ交換を必要とするプロジェクトの実施時や調達業務の実施時に必要となる複数閉域網向けの共用サーバの構築、運用などを提供するハウジングサービスが展開できる。このサービスを利用することで、ユーザは自社の閉域網を変更せず、また、閉域性を失う事なく容易にプロジェクト毎に一時的に必要となる共用サーバの運用ができ、複数の企業と連携して行うプロジェクトの情報化がスムーズに行えるので、この発明により実現されるサービスは、現在ISP(Internet Service Provider)が行っているVPN(Virtual Private Network)サービスの新しい付加サービスとしての展開が見込める。また、この方法により実現されるサーバ側から閉域網のホストへの閉域性を維持しての接続確立が可能であることを利用して、サーバ側ネットワークに複数の閉域網で提供されている種々のサービスを統合的に利用できるサーバを構築し、個人向けのポータルサイトサービスの展開も可能になる。このように、この発明は閉域網向けの新しい情報流通プラットフォームを構築する手段としての利用が見込める。

【図面の簡単な説明】

【図1】第1発明を適用したシステムの構成例を示す図。

【図2】Aは図1中のR-NATにおけるアドレス変換テーブルの例を示す図、Bは各閉域網に対する、サーバ側ネットワークのアドレス空間の割り当て例を示す図である。

【図3】ホスト1についてのパケットの変換の様子を示す図。

【図4】ネットワークアドレス変換のイメージを示す図。

28

【図5】閉域網に割り当てられたネットワークアドレス空間の利用方針を示す図。

【図6】パケットにおけるアドレス変換の様子を示す図。

【図7】第1発明と従来技術との特徴の関係を示す図。

【図8】第2発明を適用したシステムの構成例を示す図。

【図9】VLANタグの割り当て例を示す図。

【図10】VNAT機能のパケットに対する動作を示す図。

【図11】VNATタグを利用したサーバ内の動作を示す図。

【図12】第2発明におけるVLANタグの対応付けの例を示す図。

【図13】第1発明の具体例におけるシステムを示す図。

【図14】図12中のR-NAT装置でのアドレス割り当ての例を示す図。

【図15】第2発明の具体例におけるシステムを示す図。

【図16】図15中のVNAT装置におけるVLANタグの割り当て例を示す図。

【図17】第2発明の変形におけるVLANタグとアドレスとPPP回線の対応を示す図。

【図18】R-NAT装置の概略機能構成を示す図。

【図19】R-NAT装置における処理の一部を示す流れ図。

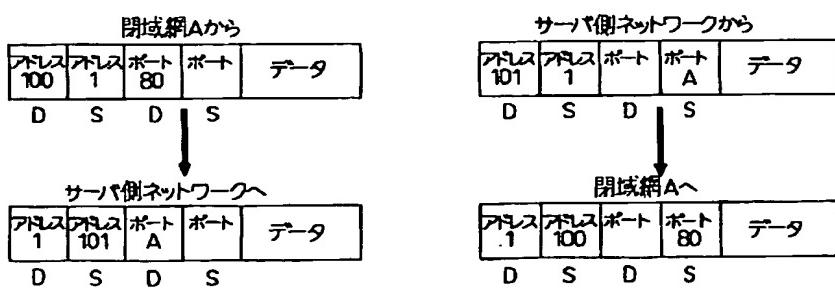
【図20】VNAT装置の概略機能構成を示す図。

【図21】VNAT装置における処理の一部を示す流れ図。

【図22】従来のPPPトンネリング接続のシステムを示す図。

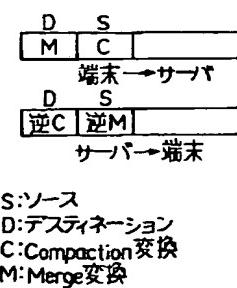
【図23】従来のNATによる接続のシステムを示す図。

【図3】



S:ソース
D:デスティネーション

【図6】

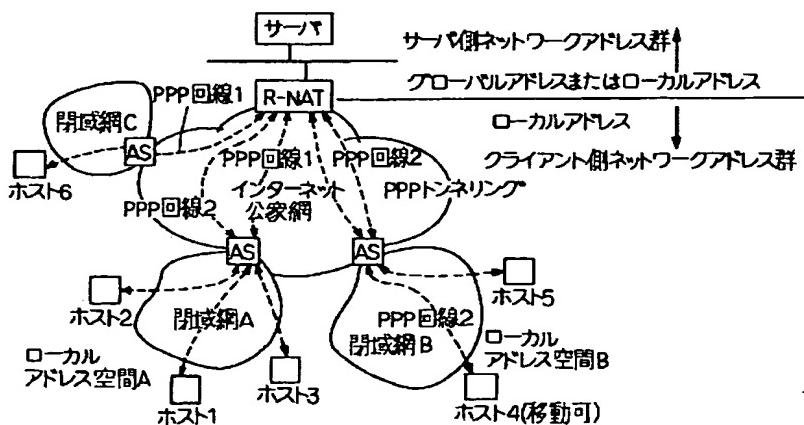


S:ソース
D:デスティネーション
C:Compaction変換
M:Merge変換

図6

図3

【図1】



R-NAT: Root-side NAT機能付きアクセスサーバ
AS: アクセスサーバ

図1

【図11】

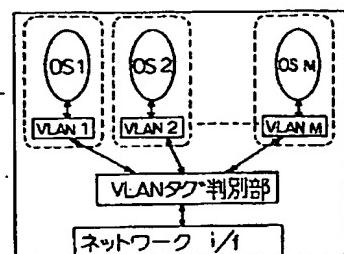


図11

【図2】

	閉域網 A	閉域網 B	サーバ側ネットワーク
ホスト1	アドレス1	—	アドレス101
ホスト2	アドレス2	—	アドレス220
ホスト3	アドレス3	—	アドレス102
ホスト4	—	アドレス11	アドレス301(静的)
ホスト5	—	アドレス22	アドレス321
Server	アドレス100	アドレス150	アドレス1

B

	閉域網 A	閉域網 B
割り当て空間	アドレス空間 101-300	アドレス空間 301-350
PPP回線 1	アドレス空間 101-200	アドレス空間 311-350
PPP回線 2	アドレス空間 201-250	アドレス 301

図2

【図16】

	閉域網 A	閉域網 B	閉域網 1
PPP回線 1	VLAN 1-1	VLAN 2-1	VLAN 3-1
PPP回線 2	VLAN 1-2	—	—

図16

【図5】

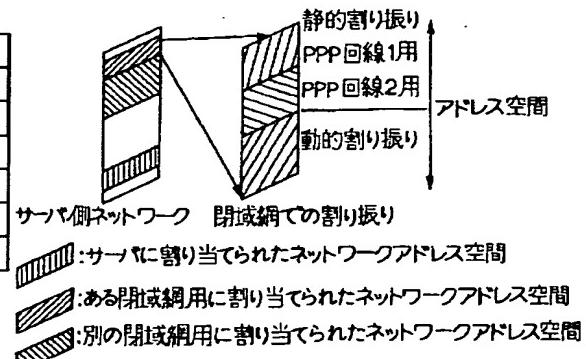


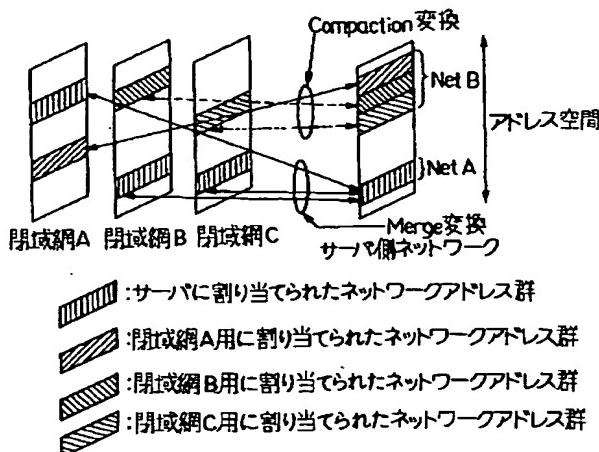
図5

【図7】

	従来のNAT	PPPトуннеинг	方法1 (Root-side NAT)
ローカルアドレスの使用	○	○	○
サーバーフラッシュ型信頼配信	×	×	○
カスタマイズドサービスの提供	△	×	○
不正アクセスパスの発生防止	×	×	○

図7

【図4】



【図8】

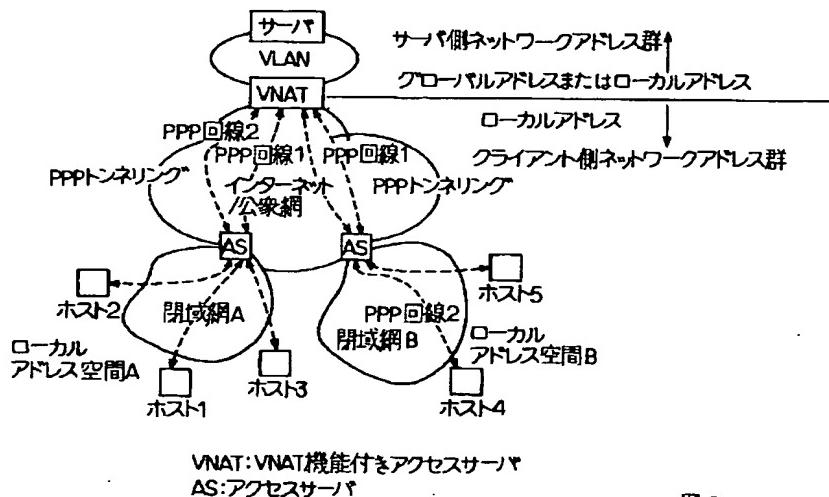


図4

【図10】

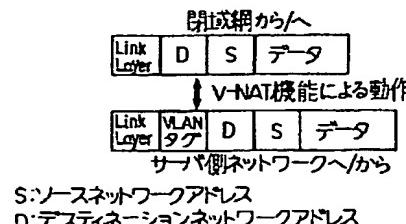


図10

【図17】

VLAN タグ	アドレス	PPP回線番号
VLAN 1	10.0.1.13	PPP回線1
VLAN 1	10.0.3.20	PPP回線2
VLAN 2	10.0.1.30	PPP回線1
VLAN 2	10.0.1.14	PPP回線1
VLAN 3	10.1.1.1	PPP回線1

図17

図8

【図9】

	閉域網 A	閉域網 B	VLAN タグ
ホスト 1	アドレス1	—	VLAN 1-1
ホスト 2	アドレス2	—	VLAN 1-2
ホスト 3	アドレス3	—	VLAN 1-1
ホスト 4	—	アドレス11	VLAN 2-2
ホスト 5	—	アドレス22	VLAN 2-1
Server	アドレス100	アドレス150	アドレス1

【図12】

VLAN タグ	ホストのアドレス	PPP回線番号
VLAN 1	アドレス1	PPP回線1
VLAN 1	アドレス2	PPP回線2
VLAN 1	アドレス3	PPP回線1
VLAN2 タグ	ホストのアドレス	PPP回線番号
VLAN2	アドレス4	PPP回線2
VLAN2	アドレス5	PPP回線1

図12

図9

【図 13】

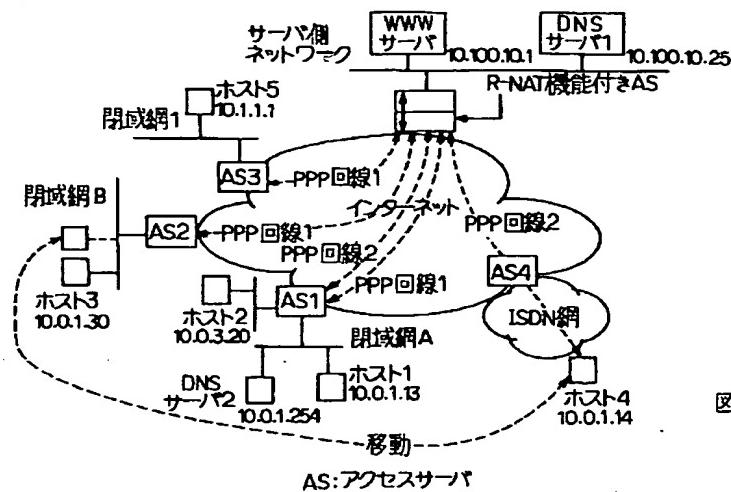


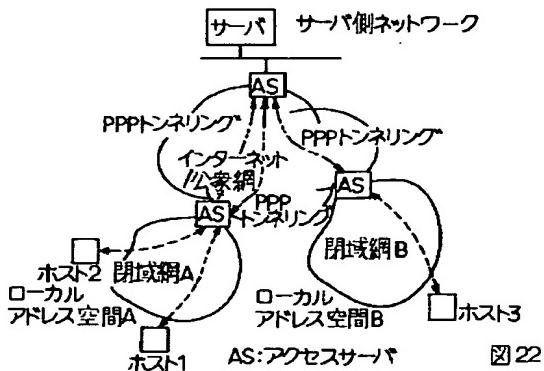
図 13

【図 14】

	閉域網 A	閉域網 B	閉域網 1	サーバ側ネットワーク
ホスト 1	10.0.1.13	—	—	10.10.1.15
ホスト 2	10.0.3.20	—	—	10.10.1.100
ホスト 3	—	10.0.1.30	—	10.10.2.10
ホスト 4	—	10.0.1.14	—	10.10.2.65
ホスト 5	—	—	10.1.1.1	10.10.11.1
Server	10.1.1.1	10.10.15.1	10.50.1.1	10.100.10.1

図 14

【図 22】



【図 15】

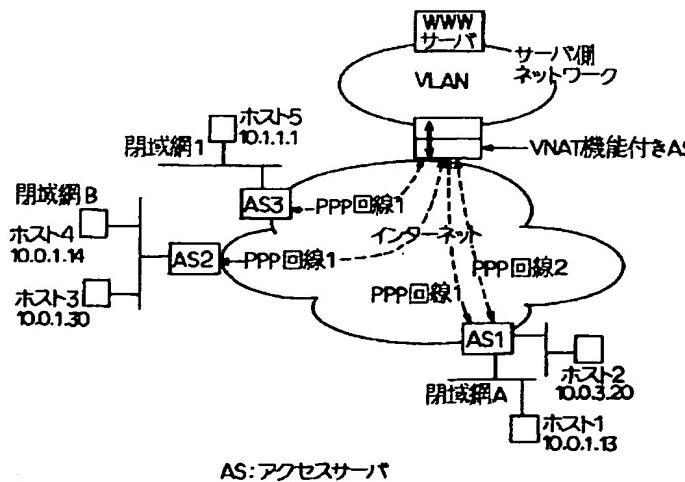


図 15

【図18】

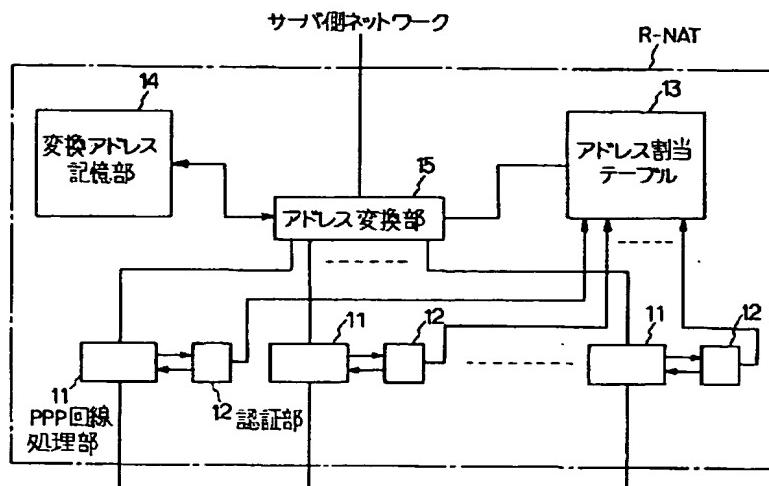


図18

【図19】

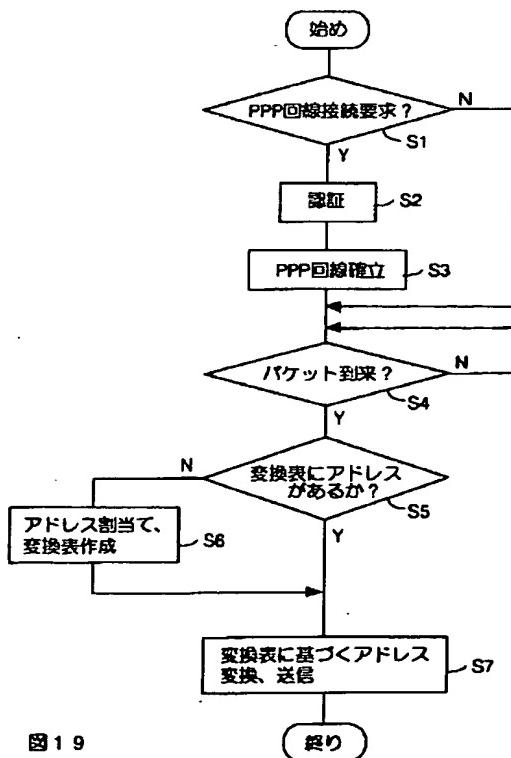


図19

【図21】

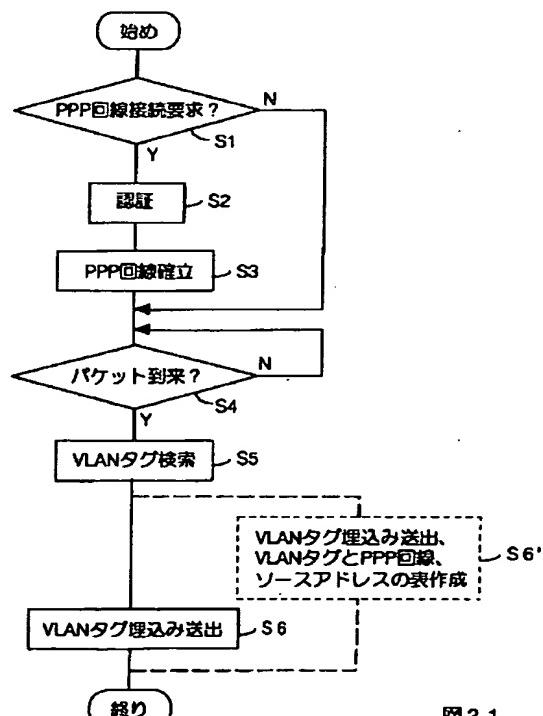


図21

【図20】

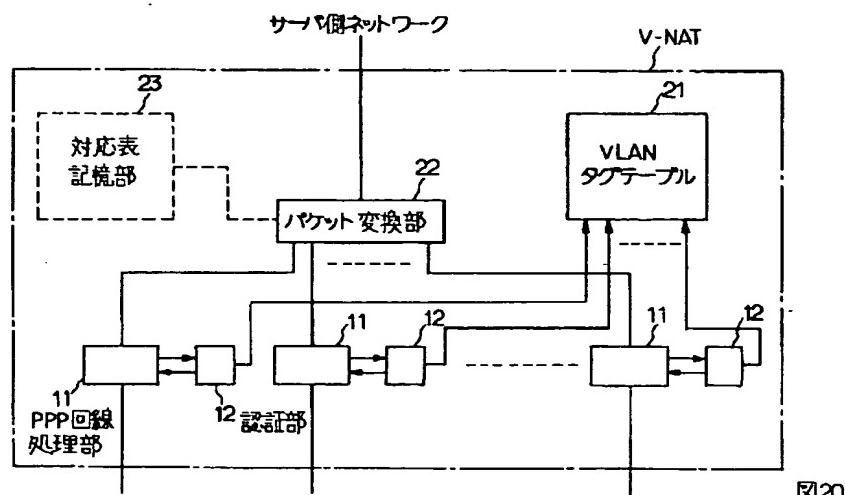


図20

【図23】

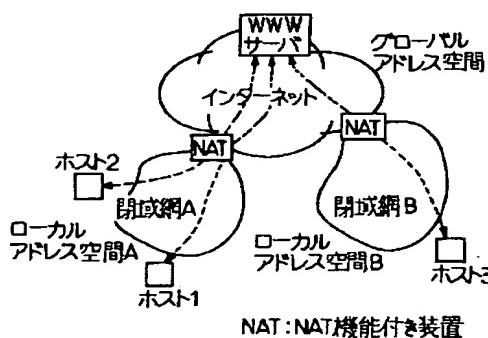


図23